Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **12** (2018), 166–177.
https://doi.org/10.2298/AADM170530005P

AN APPLICATION OF BIVARIATE POLYNOMIAL FACTORIZATION ON DECODING OF REED-SOLOMON BASED CODES

*Ivan Pavkov, Nebojša M. Ralević, Ljubo Nedović**

A necessary and sufficient condition for the existence of a non-trivial factorization of an arbitrary bivariate polynomial with integer coefficients was presented in [**2**]. In this paper we develop an efficient algorithm for factoring bivariate polynomials with integer coefficients. Also, we shall give a proof of the optimality of the algorithm. For a given codeword, formed by mixing up two codewords, the algorithm recovers those codewords directly by factoring corresponding bivariate polynomial. Our algorithm determines uniquely the given polynomials which are used in forming the mixture of two codewords.

1. INTRODUCTION

Error-correcting codes enable reliable transmission over a noisy communication channel. The idea is to encode the message to be transmitted into a longer, redundant string, called a codeword, and then transmit the codeword over the noisy channel. The redundancy is chosen in order to enable the receiver to decode the transmitted codeword even from a somewhat distorted version of the codeword.

Reed-Solomon codes are examples of error-correcting codes, in which redundant information is added to data so that it can be recovered reliably despite errors in transmission or storage and retrieval. Reed-Solomon codes were used in several of NASA and ESA's planetary exploration missions. Reed-Solomon codes are

*Corresponding author. Ljubo Nedović
2010 Mathematics Subject Classification. 12Y05,
Keywords and Phrases. Bivariate polynomials, Decoding, Newton polygon, Non-trivial factorization, Reed-Solomon code.

widely studied in literature, even in some recently published papers (e.g. [**7**] and [**8**]).

Irreducibility of bivariate polynomials with integer coefficients as well as their polynomial factorization were studied in [**1**],[**2**], [**3**] and [**4**].

We present an algorithm that, for a given received word, formed by mixing up two codewords (see [**5**]), recovers those codewords directly by factoring the corresponding bivariate polynomial.

2. PRELIMINARIES

We start with the necessary definition and results. For more details see [**2**].

Definition 2.1 The *convex hull* of a set S in $\mathbb{R}^2$ (denoted by $conv(S)$) is the smallest convex set that contains the set S.

Definition 2.2 For two arbitrary sets $A, B \subset \mathbb{R}^2$, the set $A + B = \{a + b : a \in A, b \in B\}$ is called the *Minkowski sum of sets* A and B.

Definition 2.3 An arbitrary point from $\mathbb{R}^2$ is called an *integer point* if both of its coordinates are integers. An arbitrary polygon in $\mathbb{R}^2$ is called an integer polygon if all of its vertices are integer points.

Definition 2.4 We say that the integer polygon C is *integrally decomposable* if there exist integer polygons A and B that satisfy $C = A + B$, with both A and B containing at least two points. Polygons A and B are called polygon summands of the polygon C. Otherwise, polygon C is integrally indecomposable, i.e., there is no non-trivial decomposition of polygon C.

Definition 2.5 Consider an arbitrary polynomial $f(x, y)$ from $\mathbb{Z}[x, y]$:

$$f(x, y) = \sum C_{e_1 e_2} x^{e_1} y^{e_2}.$$

Consider an exponent vector (e_1, e_2) as a point in $\mathbb{Z}^2$. The *Newton polygon of the polynomial* $f(x, y)$, denoted by P_f, is defined as the convex hull in $\mathbb{R}^2$ of all the points (e_1, e_2) with $C_{e_1 e_2} \in \mathbb{Z} \setminus \{0\}$.

Definition 2.6 Let $f(x, y) \in \mathbb{Z}[x, y]$. The *non-extended lattice of nodes* of the polynomial $f(x, y)$ consists of all the points $(e_1, e_2)_i$, $i = 1, ..., k$ corresponding to the terms with non-zero coefficients. If the Newton polygon of $f(x, y)$ contains some integer points different from $(e_1, e_2)_i$, $i = 1, ..., k$, these points, together with $(e_1, e_2)_i$, $i = 1, ..., k$, form an *extended lattice of nodes*.

Example 2.1 Consider a polynomial $f(x, y)$ in $\mathbb{Z}[x, y]$:

$$f(x, y) = 3x^2y^2 + 2xy^2 + x^2 + 1.$$

Non-zero terms correspond to the points $(2, 2)$, $(1, 2)$, $(2, 0)$ and $(0, 0)$. These points form the non-extended lattice of nodes of the polynomial $f(x, y)$ shown in Figure 1.

The Newton polygon of the polynomial $f(x,y)$ is the convex hull of $(2,2)$, $(1,2)$, $(2,0)$ and $(0,0)$, denoted as $conv\{(2,2),(1,2),(2,0),(0,0)\}$ shown in Figure 2.

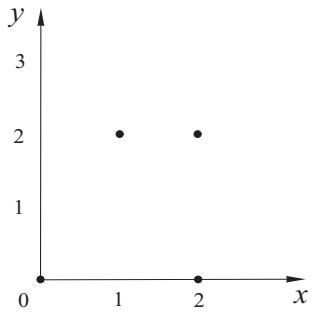

Figure 1.

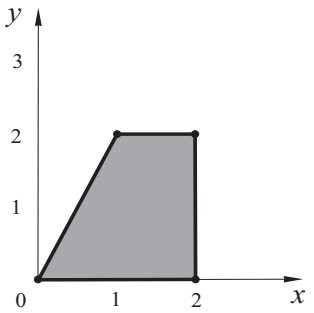

Figure 2.

The Newton polygon of the polynomial $f(x,y)$ also captures integer points $(1,0)$, $(1,1)$ and $(2,1)$, as shown in Figure 3.

The points from the non-extended lattice of nodes together with points $(1,0)$, $(1,1)$ and $(2,1)$ form the extended lattice of nodes shown in Figure 4.

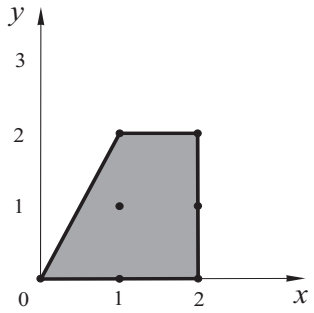

Figure 3.

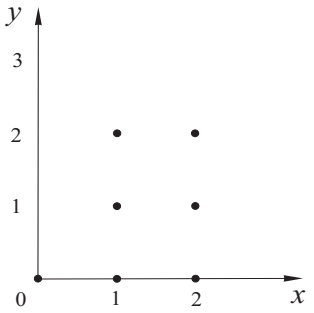

Figure 4.

Theorem 2.1 *Let F be an arbitrary field. Let $f(x,y), g(x,y), h(x,y) \in F[x,y]$, with $f(x,y) \neq 0$ and $f(x,y) = g(x,y)h(x,y)$. Then $P_f = P_g + P_h$.*

Theorem 2.2 *Let $f(x,y)$ be a non-zero bivariate polynomial over an arbitrary field F, non-divisible either by x or by y. If the Newton polygon of the polynomial $f(x,y)$ is integrally indecomposable, then $f(x,y)$ is absolutely irreducible over F.*

Definition 2.7 Let $f(x,y)$ be a polynomial from $\mathbb{Z}[x,y]$. Let $P = \{A_1, A_2, ..., A_n\}$ be the lattice of nodes of the polynomial $f(x,y)$ possibly extended by some integer points that lie inside of the Newton polygon of the polynomial $f(x,y)$ or on its edge. Without loss of generality, we can assume that after the construction of the Newton polygon of $f(x,y)$, $A_1, A_2, ..., A_k$, $k \geq 2$, become its vertices, and $A_{k+1}, ..., A_n$ do not. We say that the grouping $G_1, ..., G_l$, $l \geq 2$, of the set P is a *super-covering* of P if:

1. Each group G_i, $i = 1, ..., l$, contains the same number of points not less than two,
2. $\bigcup_{i=1}^{l} G_i = P$,
3. Points $A_1, A_2, ..., A_k$ appear in exactly one of the sets $G_1, ..., G_l$,
4. Points $A_{k+1}, ..., A_n$ appear in at least one of the sets $G_1, ..., G_l$,
5. Convex polygons $G_2, ..., G_l$ are obtained from G_1 by translation.

Definition 2.8 Let $f(x, y)$ be a polynomial in $\mathbb{Z}[x, y]$. Let $P = \{A_1, A_2, ..., A_n\}$ be the lattice of nodes of the polynomial $f(x, y)$ possibly extended by some integer points from the inner area of the Newton polygon or its edge. Let $G_1 = conv(A_{i_{1,1}}, ..., A_{i_{1,k}}), ..., G_l = conv(A_{i_{l,1}}, ..., A_{i_{l,k}}), l \geq 2$, where $\{i_{1,1}, ..., i_{1,k}, ..., i_{l,1}, ..., i_{l,k}\} = \{1, ..., n\}$ be a super-covering of P by l congruent $k-$gons. Due to the fact that the composition of two translations is also a translation, we conclude that, for any of the G_p and G_q, $p \neq q$, $p, q \in \{1, ..., l\}$ there exists a translation $\tau_{p,q}$, such that $\tau_{p,q}(G_p) = G_q$. For each polygon, we list vertices in such a way that we firstly list the vertex with the smallest $x-$coordinate. If such vertex is not unique, we choose the one having simultaneously the smallest $y-$coordinate.

Then we list the other vertices in counterclockwise order. It is clear that $\tau_{p,q}(A_{i_{p,w}}) = A_{i_{q,w}}$, for any of the p and q, $p \neq q$, $p, q \in \{1, ..., l\}$ and each $w = 1, ..., k$. Let us denote by $coef(A_i)$ the coefficient of the monomial of the polynomial $f(x, y)$ corresponding to the exponent vector A_i. Assume that polygons $G_1, G_2, ..., G_l$ have no common node. We say that the super-covering of P is *suitable super-covering with respect to the coefficients of the polynomial* $f(x, y)$ if

$$coef(A_{i_{1,1}}) : coef(A_{i_{1,2}}) : ... : coef(A_{i_{1,k}}) = ... = coef(A_{i_{l,1}}) : coef(A_{i_{l,2}}) : ... : coef(A_{i_{l,k}}).$$

Assume that polygons $G_1, ..., G_l$ have common nodes. Each G_i, $i = 1, ..., l$, determines a polynomial $p_i(x, y)$ such that $f(x, y) = p_1(x, y) + ... + p_l(x, y)$, where polynomial summands $p_i(x, y)$, $i = 1, ..., l$, are ordered in the same way as the vertices. For each node A_c that is common for s polygons, the coefficient of the monomial whose exponent vector is A_c is partitioned into s summands such that every summand belongs to one and only one $p_i(x, y)$, corresponding to the polygons having a common node A_c and the coefficients of $p_1(x, y)$,...,$p_l(x, y)$, $p_i(x, y) = c_{i,1}x^{\alpha_{i,1}}y^{\beta_{i,1}} + ... + c_{i,k}x^{\alpha_{i,k}}y^{\beta_{i,k}}$, are proportional, i.e.

$$c_{1,1} : c_{1,2} : ... : c_{1,k} = ... = c_{l,1} : c_{l,2} : ... : c_{l,k}.$$

If the above holds for every common node, we say that the super-covering is *suitable*.
Remark: If some of the points $A_{k+1}, ..., A_n$ are interior points of G_1 then they are mapped by translations to the corresponding points of $G_2, ..., G_l$.

The previous definition, because of the simplicity, is given for the cases without interior points. However, the proportions hold for the interior points also.

In the case of interior points, we list those interior points together with vertices of the polygon as arguments of *conv*.

The following theorem is from [**2**].

Theorem 2.3 *Let $f(x,y)$ be a non-zero polynomial in $\mathbb{Z}[x,y]$. Polynomial $f(x,y)$ has non-trivial integer factorization if and only if its lattice of nodes, possibly extended by some integer points captured by the Newton polygon of the polynomial $f(x,y)$, has suitable super-covering with respect to the coefficients of $f(x,y)$.*

Remark: Under the same conditions as in the previous theorem, the same holds if we consider the polynomial with rational coefficients.

Example 2.2 Consider a polynomial $f(x,y) = x^6y^6+x^4y^6+2x^4y^4+x^6y^4+x^5y^5+x^2y^6+y^6+y^4+2x^2y^4+xy^5+2x^2y^2+2x^4y^2+x^3y^3+y^2+1+x^2+xy+x^6y^2+x^4+x^6+x^5y$ over $\mathbb{Z}$. Non-zero monomials of the polynomial $f(x,y)$ correspond to the points $(6,6),(4,6),\ (4,4),\ (6,4),(5,5),(2,6),\ (0,6),(0,4),(2,4),(1,5),(2,2),(4,2),(3,3),\ (0,2),\ (0,0),\ (2,0),(1,1),\ (6,2),(4,0),(6,0)$ and $(5,1)$ The lattice of nodes of the polynomial $f(x,y)$ is shown in Figure 5.

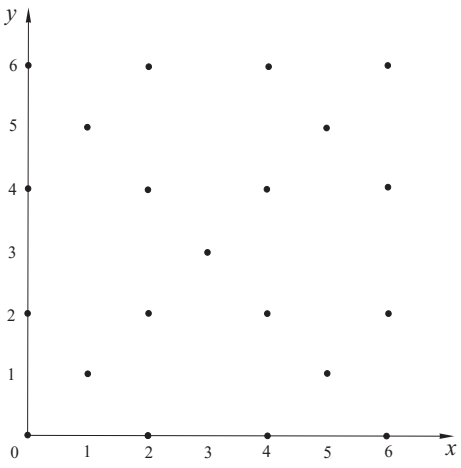

Figure 5.

Consider a square (with inner point $(1,1)$):

$$conv\{(0,0),(2,0),(2,2),(0,2),(1,1)\}$$

and its images by translation:

$$conv\{(4,0),(6,0),(6,2),(4,2),(5,1)\},$$

$$conv\{(2,2),(4,2),(4,4),(2,4),(3,3)\},$$

$$conv\{(0,4),(2,4),(2,6),(0,6),(1,5)\}$$

and

$$conv\{(4,4),(6,4),(6,6),(4,6),(5,5)\}.$$

It is obvious that this is a super-covering of the lattice of nodes shown in Figure 6.

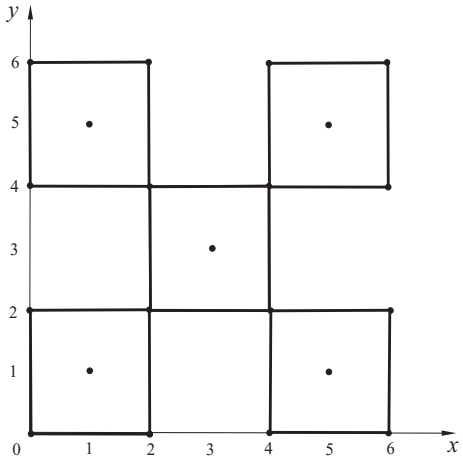

Figure 6.

Let us group monomials of $f(x,y)$ in the way induced by the super-covering: $f(x,y) = (1 + x^2 + cx^2y^2 + y^2 + xy) + (x^4 + x^6 + x^6y^2 + dx^4y^2 + x^5y) + ((2 - c)x^2y^2 + (2 - d)x^4y^2 + ex^4y^4 + fx^2y^4 + x^3y^3) + (y^4 + (2 - f)x^2y^4 + x^2y^6 + y^6 + xy^5) + ((2-e)x^4y^4 + x^6y^4 + x^6y^6 + x^4y^6 + x^5y^5$.
As proportion:$1 : 1 : c : 1 : 1 = 1 : 1 : 1 : d : 1 = (2 - c) : (2 - d) : e : f : 1 = 1 : (2 - f) : 1 : 1 : 1 = (2-e) : 1 : 1 : 1 : 1$, holds for $c = d = e = f = 1$, the super-covering shown in Figure 6. is suitable.

Further it follows:

$f(x,y) = (1+x^2+x^2y^2+y^2+xy)+(x^4+x^6+x^6y^2+x^4y^2+x^5y)+(x^2y^2+x^4y^2+x^4y^4 +x^2y^4+x^3y^3)+(y^4+x^2y^4+x^2y^6+y^6+xy^5)+(x^4y^4+x^6y^4+x^6y^6+x^4y^6+x^5y^5)$.

Thus:

$f(x,y) = (1 + x^2 + x^2y^2 + y^2 + xy) + x^4(1 + x^2 + x^2y^2 + y^2 + xy) + x^2y^2(1 + x^2 + x^2y^2 + y^2 + xy) + y^4(1 + x^2 + x^2y^2 + y^2 + xy) + x^4y^4(1 + x^2 + x^2y^2 + y^2 + xy)$
$= (1 + x^4 + x^2y^2 + y^4 + x^4y^4)(1 + x^2 + x^2y^2 + y^2 + xy)$.

3. ALGORITHM

We present an algorithm that computes the suitable super-covering of the lattice of nodes A for a given bivariate polynomial f. The algorithm iteratively tries to cover the points in A by points in a set B containing i points, $i \geq 2$, for increasing i, and in this way determines sets G_i.

1. read(A);
/*$A = \{A_i[x[i], y[i], a[i]] : i = 1, ..., n\}$, where $x[i]$ and $y[i]$ are coordinates of the lattice points, and $a[i]$ is the coefficient of the corresponding monomial.*/
2. sort(A);
/*Points $A_i \in A$ are sorted in the lexicographic order, first with respect to $x[i]$ and then to $y[i]$.*/
3. convexhull($A, ExtA$);
/*$ExtA = \{ExtA_j[xx[j], yy[j], aa[j]]\}$, are the points of the extended lattice of nodes of f. For each $A_j \in AA = ExtA \setminus A$, $x[j]$ and $y[j]$ are its coordinates, and $a[j] = 0$.*/
4. sort($ExtA$);
5. sort(AA);

6. for($cover := 0, m := 2; cover = 0, m < n; m := m + 1$);
6.1 form(B);
/*$B = \{B_j[bx[j], by[j], ba[j]] : j = 1, ..., m\}$, $B_1 \equiv A_1$, B_j, $2 \leq j \leq m$ are lattice points from A sorted lexicographically; $ba[j] := aa[j], ..., 2, 1$ if B_j is not an extreme point, and $ba[j] := aa[j]$ if B_j is an extreme point*/
6.2. covering(A, B);
/*$C = \{B_1\}$ (points in C define G_i); $D = A \setminus B$;
repeat
Find the lexicographically smallest point X from D and translate B by $\overrightarrow{B_jX}$, $j = 1, 2, ..., m$. If τB_j lie inside A and the corresponding coefficients a and ba are proportional, then τB_1 is added to C and the coefficients of points A_{jj} from τB are updated: $a[jj] := a[jj] - ba[j]$, if $a[jj] = 0$, then $D = D \setminus \{A_{jj}\}$
If for some B_j, X is not covered, then change B_j. If X is not covered for any j, then go to step 6.1 and change coefficients $ba[j]$.
until $D = \emptyset$. */
7. If $D = \emptyset$, then $cover := 1$ and go to step 8, else $cover := 0$.
8. write($cover, B, C$).
/*if $cover = 0$, the output message is that there is no coverage, and if $cover = 1$, the output is the set of points B by which we cover the initial set and it defines one factor of the polynomial, and the set of points C defines the other factor, etc*/

Theorem 3.4 *Let $f(x, y)$ be a bivariate polynomial with integer coefficients. Let $P = \{A_1, A_2, ..., A_n\}$ be the lattice of nodes of the polynomial $f(x, y)$ possibly extended by some integer points that lie inside the Newton polygon or on its edge. Let $G_1 = conv(A_{i_{1,1}}, ..., A_{i_{1,k}})$, ..., $G_l = conv(A_{i_{l,1}}, ..., A_{i_{l,k}})$, $l \geq 2$, with $\{i_{1,1}, ..., i_{1,k}, ..., i_{l,1}, ..., i_{l,k}\} = \{1, ..., n\}$ be a suitable super-covering of P by l congruent $k-$gons.*

Let $G_2 = \tau_2(G_1)$,...,$G_l = \tau_l(G_1)$. Then $conv(A_{i_{1,1}}, \tau_2(A_{i_{1,1}}), ..., \tau_l(A_{i_{1,1}}))$, ..., $conv(A_{i_{1,k}}, \tau_2(A_{i_{1,k}}), ..., \tau_l(A_{i_{1,k}}))$ is also a suitable super-covering of P by k congruent $l-$gons.

Proof. Let $G_1 = conv(A_{i_{1,1}}, ..., A_{i_{1,k}})$, ..., $G_l = conv(A_{i_{l,1}}, ..., A_{i_{l,k}})$, $l \geq 2$, be a super-covering of P by l congruent $k-$gons. If we denote $c_{i_{j,k}} = coef(A_{i_{j,k}})$, then we have:

$$c_{i_{1,1}} : c_{i_{1,2}} : ... : c_{i_{1,k}} = ... = c_{i_{l,1}} : c_{i_{l,2}} : ... : c_{i_{l,k}}.$$

Clearly, if there exists a node that is common for two or more polygons, the corresponding coefficient is partitioned in a way that such proportionality is obtained. It is obvious that:

$$conv(A_{i_{1,1}}, \tau_2(A_{i_{1,1}}), ..., \tau_l(A_{i_{1,1}})), ..., conv(A_{i_{1,k}}, \tau_2(A_{i_{1,k}}), ..., \tau_l(A_{i_{1,k}}))$$

is a super-covering of P.

Due to the fact that proportion

$$c_{i_{1,1}} : c_{i_{2,1}} : ... : c_{i_{l,1}} = ... = c_{i_{1,k}} : c_{i_{2,k}} : ... : c_{i_{l,k}},$$

also holds, this super-covering of P is suitable. □

Remark: From the previous theorem it follows that each suitable super-covering of the lattice of nodes of a polynomial $f(x, y)$ by l congruent $k-$gons uniquely determines another suitable super-covering of that lattice of nodes by k congruent $l-$gons (called dual suitable super-covering).

Remark: The algorithm presented above, starting with congruent line segments, congruent triangles etc., under the condition that a suitable super-covering of the lattice of nodes of $f(x, y)$ by l congruent k-gons exists with $k \leq l$, will reach such suitable super-covering before the suitable super-covering with k congruent $l-$gons. In other words, this means that the algorithm described in this section is optimal.

4. AN APPLICATION ON REED-SOLOMON CODES

The well known application of bivariate polynomial factorization in coding theory is presented in [**6**]. In this section we introduce an algorithm that for a given codeword which is a mixture of two codewords, recovers those codewords directly by factoring the corresponding bivariate polynomial.

Definition 4.9 Let $m_0, m_1, m_2, ..., m_{k-1} \in GF(n)$ be a $k-$tuple of elements from $GF(n)$. Let α be a primitive element of the field $GF(n)$. A Reed-Solomon codeword c is formed by evaluating polynomial $p(x) = m_0 + m_1 x + m_2 x^2 + ... + m_{k-1} x^{k-1}$ for each of the n elements in the $GF(n)$:

$$c = (c_0, c_1, c_2, ..., c_{n-1}) = (p(0), p(\alpha), p(\alpha^2), ..., p(\alpha^{n-1})).$$

A complete set of codewords is constructed by taking all different $k-$tuples $(m_0, m_1, m_2, ..., m_{k-1})$ from the field $GF(n)$.

Remark: Since there are n^k different $k-$tuples in $GF(n)$, the Reed-Solomon code has n^k codewords.

Definition 4.10 Code is *linear* if the sum of any two codewords is also a codeword.

Remark: As the sum of two polynomials of degree $(k-1)$ is another polynomial of degree at most $(k-1)$, Reed-Solomon codes are linear.

Remark: It is easy to prove that Reed-Solomon codewords form a vector space of dimension k over $GF(n)$. The number k is called the dimension of the code. Number n is called the length of the code. Therefore Reed-Solomon codes, as any other linear code, are denoted as (n, k) codes.

Venkatesan Guruswami introduces a mixture of two codewords in [**5**].

Definition 4.11 Let n be a prime number and let $GF(n)$ be a finite field of characteristic n. Let $(m_0, m_1, m_2, ..., m_{k-1})$ and $(d_0, d_1, d_2, ..., d_{k-1})$, $m_0, m_1, m_2, ..., m_{k-1}$, $d_0, d_1, d_2, ..., d_{k-1} \in GF(n)$ be two $k-$tuples of elements from $GF(n)$. Let $p_1(x) = m_0 + m_1 x + m_2 x^2 + ... + m_{k-1} x^{k-1}$ and $p_2(x) = d_0 + d_1 x + d_2 x^2 + ... + d_{k-1} x^{k-1}$. Let c_1 and c_2 be Reed-Solomon codewords corresponding to the polynomials p_1

and p_2. *Mixture of codewords* c_1 and c_2 corresponds to the bivariate polynomial $q(x,y) = y^2 - s(x)y + p(x)$, with $s(x) = p_1(x) + p_2(x)$ and $p(x) = p_1(x) \cdot p_2(x)$.

Remark: It is obvious that polynomial $q(x,y)$ has a unique factorization in the form $q(x,y) = (y - p_1(x))(y - p_2(x))$. Therefore we suggest finding $p_1(x)$ and $p_2(x)$ directly by factoring bivariate polynomial $q(x,y)$ by the algorithm described above, as it is shown in the following example.

Example 4.3 Let $(1,0,3,1,2)$ and $(2,2,0,3,1)$ be two 5−tuples of elements from $\mathbb{Z}_5$ and let $p_1(x) = 1 + 3x^2 + x^3 + 2x^4$ and $p_2(x) = 2 + 2x + 3x^3 + x^4$ be the corresponding polynomials. Let c_1 and c_2 be the codewords corresponding to the polynomials $p_1(x)$ and $p_2(x)$. The mixture of the codewords c_1 and c_2 corresponds to the bivariate polynomial:

$q(x,y) = y^2 - ((1+3x^2+x^3+2x^4)+(2+2x+3x^3+x^4))y + (1+3x^2+x^3+2x^4)(2+2x + 3x^3 + x^4) = y^2 - 3y - 2xy - 3x^2y - 4x^3y - 3x^4y + 2 + 2x + 6x^2 + 11x^3 + 7x^4 + 13x^5 + 6x^6 + 7x^7 + 2x^8$.

As the coefficients are from the finite field $\mathbb{Z}_5$, $q(x,y)$ has a form:

$$q(x,y) = y^2 - 3y - 2xy - 3x^2y - 4x^3y - 3x^4y + 2 + 2x + x^2 + x^3 + 2x^4 + 3x^5 + x^6 + 2x^7 + 2x^8.$$

Non-zero terms of $q(x,y)$ correspond to the points $(0,2),(0,1),(1,1),(2,1),(3,1),$ $(4,1),$ $(0,0),(1,0),(2,0),$ $(3,0),$ $(4,0),$ $(5,0),$ $(6,0),(7,0),(8,0)$. The lattice of nodes of $q(x,y)$ is shown in Figure 7.
It is obvious that there is no super-covering of the lattice with line segments.

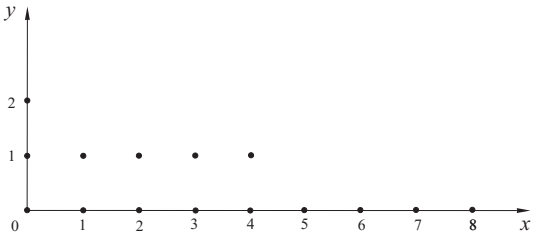

Figure 7.

A super-covering of the lattice by $conv\{(0,1),(0,0),(1,0),(2,0),(3,0),(4,0)\}$, and its images by translation $conv\{(0,2),(0,1),(1,1),(2,1),(3,1),(4,1)\}$, and

$$conv\{(4,1),(4,0),(5,0),(6,0),(7,0),(8,0)\}$$

is shown in Figure 8.

Nodes $(1,0),$ $(2,0),$ $(3,0),$ $(1,1),$ $(2,1),$ $(3,1),$ $(5,0),$ $(6,0)$ and $(7,0)$ belong to only one of the polygons and nodes $(1,0),(2,0),(3,0)$ are mapped by translation to $(1,1),(2,1),(3,1)$ and $(5,0),(6,0),(7,0)$ in that order.

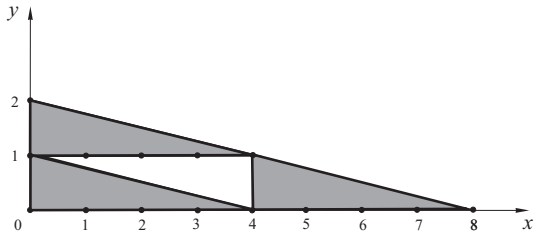

Figure 8.

As proportion: $2:1:1=(-2):(-3):(-4)=3:1:2$, does not hold, the super-covering is not suitable.

Consider a super-covering of the lattice by $conv\{(0,1),(0,0),(1,0),(3,0),(4,0)\}$ (shown in Figure 9.) and its images by translation:

$$conv\{(0,2),(0,1),(1,1),(3,1),(4,1)\},$$

$$conv\{(2,1),(2,0),(3,0),(5,0),(6,0)\},$$

$$conv\{(3,1),(3,0),(4,0),(6,0),(7,0)\},$$

$$conv\{(4,1),(4,0),(5,0),(7,0),(8,0)\}.$$

Let us group monomials of $q(x,y)$ in the way induced by the super-covering:

$q(x,y) = (ay+2+2x+bx^3+dx^4)+(y^2+(-3-a)y-2xy+fx^3y+gx^4y)+(-3x^2y+x^2+cx^3+hx^5+vx^6)+((-4-f)x^3y+(1-b-c)x^3+ex^4+(1-v)x^6+wx^7)+((-3-g)x^4y+(2-d-e)x^4+(3-h)x^5+(2-w)x^7+2x^8)$.

Due to the fact that coefficients of the polynomial are from $\mathbb{Z}_5$, all the coefficients should be considered modulo 5 in order to obtain proportionality. Choosing:

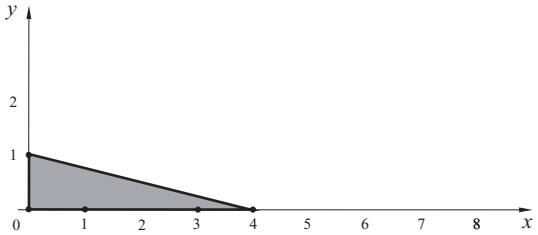

Figure 9.

$q(x,y)=(ay+2+2x+bx^3+dx^4)+(y^2+(-3-a)y-2xy+fx^3y+gx^4y)+(-3x^2y+6x^2+cx^3+hx^5+vx^6)+((-4-f)x^3y+(11-b-c)x^3+ex^4+(6-v)x^6+wx^7)+((-3-g)x^4y+(7-d-e)x^4+(13-h)x^5+(7-w)x^7+2x^8)$,
the proportionality of coefficients is achieved for $a=-1$, $c=6$, $b=3$, $d=1$, $f=-3$, $g=-1$, $h=9$, $v=3$, $e=2$ and $w=1$.

Further we get:

$$q(x,y)=(-y+2+2x+3x^3+x^4)+(y^2-2y-2xy-3x^3y-x^4y)+(-3x^2y+6x^2+6x^3+9x^5$$

$$+3x^6)+(-x^3y+2x^3+2x^4+3x^6+x^7)+(-2x^4y+4x^4+4x^5+6x^7+2x^8)$$

$$=-(y-2-2x-3x^3-x^4)+y(y-2-2x-3x^3-x^4)-3x^2(y-2-2x-3x^3-x^4)$$

$$-x^3(y-2-2x-3x^3-x^4)-2x^4(y-2-2x-3x^3-x^4).$$

Finally, $q(x,y)=(-1+y-3x^2-x^3-2x^4)(y-2-2x-3x^3-x^4)$, i.e.,

$$q(x,y)=(y-(1+3x^2+x^3+2x^4))(y-(2+2x+3x^3+x^4)).$$

It follows that $p_1(x)=1+3x^2+x^3+2x^4$ and $p_2(x)=2+2x+3x^3+x^4$.

Acknowledgment. The second and third author acknowledge the financial support of the Ministry of Education, Science and Technological Development of the Republic of Serbia, in the frame of Project applied under No. 34014. The second author acknowledge the financial support of the Ministry of Education, Science and Technological Development of the Republic of Serbia, in the frame of Project applied under No. 174009.

REFERENCES

1. F. Abu Salem, S. Gao, A. G. B. Lauder: *Factoring polynomials via polytopes: extended version.* Report PRG-RR-04–07, Oxford University Computing Laboratory, (2004)
2. S. Crvenković, I. Pavkov: *Factoring bivariate polynomials with integer coeficients via Newton polygons.* Filomat 27:2 (2013), 215–226.
3. S. Gao: *Absolute irreducibility of polynomials via Newton polytopes.* Journal of Algebra 237, No.2 (2001) 501–520.
4. S. Gao, A.G.B. Lauder: *Decomposition of polytopes and polynomials.* Discrete and Computational Geometry 26 (2001) 89–104.
5. V. Guruswami: *Algorithmic Results in List Decoding.*Foundations and Trends in Theoretical Computer Science Vol. 2, No. 2(2006), 107–195.
6. M. Sudan: *Decoding of Reed Solomon Codes beyond the Error-Correction Bound.* Journal of Complexity 13 (1997), 180–193.
7. V. Gandikota, B. Ghazi, E. Grigorescu: *NP-Hardness of Reed-Solomon Decoding and the Prouhet-Tarry-Escott Problem.* 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (2016), 760–769.
8. K. Mergu: *Performance Analysis of Reed-Solomon Codes Concatenated with Convolutional Codes over AWGN Channel.* APTIKOM Journal on Computer Science and Information Technologies, Vol. 1, No. 1, (2016), 27–32.

Ivan Pavkov
Novi Sad Business School,
Higher education institution
for applied studies,
Vladimira Perića-Valtera 4,
21000 Novi Sad,
Serbia,
e-mail: *pavkov.ivan@gmail.com*

Nebojša M. Ralević
University of Novi Sad,
Faculty of Technical Sciences,
Department of Mathematics,
Trg Dositeja Obradovića 6,
21000 Novi Sad,
Serbia,
e-mail: *nralevic@uns.ac.rs*

Ljubo Nedović
University of Novi Sad,
Faculty of Technical Sciences,
Department of Mathematics,
Trg Dositeja Obradovića 6,
21000 Novi Sad,
Serbia,
e-mail: *nljubo@uns.ac.rs*

(Received 30.05.2017.)
(Revised 14.10.2017.)